ASCAP

ASCAP
Agjencia e Sigurimit të Cilësisë së Arsimit Parauniversitar

MODUL KURRIKULAR

Kurrikula në Bazë Shkolle ose me Zgjedhje në Arsimin e Mesëm të Lartë

SIGURIA KIBERNETIKE DHE QYTETARIA DIGJITALE

Koordiantor: Eriksen Mersinllari

www.ascap.edu.al

2026

MODUL KURRIKULAR

KURRIKULA NË BAZË SHKOLLE / ME ZGJEDHJE NË ARSIMIN E MESËM TË LARTË

"SIGURIA KIBERNETIKE DHE QYTETARIA DIGJITALE"

I. HYRJE

Moduli kurrikular "***Siguria kibernetike dhe qytetaria digjitale***" është hartuar në përputhje me parimet dhe drejtimet themelore të Kornizës Kurrikulare të Arsimit Parauniversitar dhe Kurrikulës Bërthamë të Arsimit të Mesëm të Lartë, të cilat vendosin në qendër zhvillimin e kompetencave kyçe, përdorimin e përgjegjshëm të teknologjisë, edukimin qytetar dhe mirëqenien e nxënësve në mjedisin digjital. Nxënësit e klasës së dhjetë janë përdorues aktivë të internetit, të rrjeteve sociale, të platformave të komunikimit, të aplikacioneve të ndryshme dhe të shërbimeve digjitale që lidhen me jetën e tyre të përditshme, me të nxënit dhe me ndërveprimin shoqëror. Në këtë fazë, ata jo vetëm konsumojnë përmbajtje digjitale, por edhe e krijojnë, e shpërndajnë dhe ndikohen prej saj. Për këtë arsye, krahas aftësive teknike, ata kanë nevojë të zhvillojnë aftësi më të thelluara për të kuptuar rreziqet që lidhen me sigurinë kibernetike, mbrojtjen e privatësisë, verifikimin e informacionit, etikën e komunikimit dhe qytetarinë digjitale.

Qëllimi i modulit është të pajisë nxënësit me njohuritë, aftësitë dhe qëndrimet e nevojshme për të përdorur teknologjinë në mënyrë të sigurt, kritike dhe etike, për të kuptuar dhe analizuar kërcënimet më të zakonshme në mjedisin online, për të mbrojtur llogaritë, të dhënat dhe pajisjet e tyre, si dhe për të reaguar në mënyrë të përgjegjshme ndaj situatave problematike në mjedisin digjital.

Në këtë kuadër, moduli synon:

- zhvillimin e të kuptuarit mbi identitetin online, gjurmën digjitale dhe ndikimin që prania në internet ka në reputacionin personal dhe shoqëror;
- njohjen dhe analizimin e kërcënimeve më të zakonshme kibernetike, si phishing-u, malware-i, profilet e rreme, manipulimi social, bullizmi kibernetik dhe cenimi i privatësisë;
- formimin e aftësive praktike për mbrojtjen e llogarive, fjalëkalimeve, të dhënave personale dhe pajisjeve digjitale;
- zhvillimin e aftësive për verifikimin e informacionit, dallimin e dezinformimit dhe përdorimin kritik të mediave dhe rrjeteve sociale;
- ndërgjegjësimin për të drejtat, përgjegjësitë dhe parimet etike që lidhen me qytetarinë digjitale dhe përdorimin e teknologjisë;

- nxitjen e reagimit të sigurt dhe të strukturuar ndaj incidenteve digjitale, përfshirë raportimin, kërkimin e ndihmës dhe ndërtimin e zakoneve të qëndrueshme të higjienës kibernetike;
- fuqizimin e nxënësve për të bashkëpunuar në nisma dhe produkte ndërgjegjësuese që promovojnë sigurinë digjitale në shkollë dhe në komunitet.

Moduli ka karakter praktik, reflektues dhe ndërdisiplinor, ai zhvillohet përmes veprimtarive si analiza rastesh, diskutime të drejtuara, simulime, punë në grup, produkte ndërgjegjësuese dhe reflektim individual, duke krijuar mundësi që nxënësit të zbatojnë njohuritë në situata të afërta me realitetin e tyre. Në këtë mënyrë, moduli nuk synon vetëm përvetësimin e informacionit, por zhvillimin e aftësisë për të menduar në mënyrë kritike, për të marrë vendime të informuara dhe për të vepruar me përgjegjësi në mjedisin digjital.

Moduli mund të zbatohet në klasën e dhjetë, duke u përshtatur me kontekstin e shkollës, interesat e nxënësve dhe zhvillimet bashkëkohore në fushën e teknologjisë dhe të sigurisë kibernetike. Në këtë kuadër, siguria kibernetike trajtohet jo vetëm si një çështje teknike, por edhe si një dimension i rëndësishëm i qytetarisë digjitale, etikës, mirëqenies dhe pjesëmarrjes së vetëdijshme në mjedisin virtual.

2. PËRMBAJTJA E MODULIT

Moduli është strukturuar në shtatë tematika të ndërlidhura, të cilat trajtojnë në mënyrë progresive aspekte të ndryshme të sigurisë kibernetike dhe qytetarisë digjitale. Përmbajtja e tij ndërtohet mbi njohuritë dhe përvojat paraprake të nxënësve në përdorimin e teknologjisë dhe mjedisit digjital, duke i thelluar ato në drejtim të identitetit dhe reputacionit online, kërcënimeve kibernetike, mbrojtjes, verifikimit të informacionit dhe etikës digjitale. Në vijim, moduli adreson reagimin ndaj incidenteve dhe përfshirjen aktive të nxënësve në veprimtari ndërgjegjësuese për komunitetin shkollor, duke kulmuar me realizimin e një produkti final me vlerë praktike dhe edukative.

Në tematikën "Ekosistemi digjital, identiteti online dhe gjurma digjitale", nxënësi analizon mënyrën se si ndërtohet dhe projektohet prania e tij në internet, duke reflektuar mbi informacionin që publikon, mbi të dhënat që ruhen, mbi audiencën që mund t'i aksesojë ato dhe mbi mënyrën se si kjo prani mund të interpretohet nga të tjerët. Në këtë kuadër, trajtohen konceptet e identitetit online, gjurmës digjitale aktive dhe pasive, reputacionit digjital dhe kufirit ndërmjet hapësirës private dhe asaj publike. Tematika synon të zhvillojë te nxënësi

kuptimin se çdo veprim në mjedisin digjital lë pasoja dhe se sjellja online ndikon drejtpërdrejt në marrëdhëniet shoqërore, mirëqenien personale dhe mundësitë e ardhshme.

Në tematikën "Kërcënimet kibernetike dhe llojet e sulmeve", nxënësi njihet me kërcënimet më të zakonshme me të cilat mund të përballet një i ri në mjedisin online, si malware, phishing, profile të rreme, mashtrime me oferta ose shpërblime, manipulimi social, bullizmi kibernetik dhe cenimi i llogarive. Përmes trajtimit të këtyre çështjeve, nxënësi aftësohet të identifikojë shenjat paralajmëruese të rrezikut, të dallojë mekanizmat dhe taktikat e manipulimit dhe të kuptojë pse faktori njerëzor përbën një nga hallkat më të ndjeshme të sigurisë digjitale.

Në tematikën "Mbrojtja e llogarive, fjalëkalimeve dhe të dhënave personale", nxënësi fokusohet në praktikat themelore të mbrojtjes së sigurisë personale në mjedisin digjital. Në këtë kuadër trajtohen çështje që lidhen me krijimin e fjalëkalimeve të forta, përdorimin e fjalëkalimeve të ndryshme për llogari të ndryshme, autentikimin me dy faktorë, përditësimin e pajisjeve, rezervimin e të dhënave, menaxhimin e lejeve të aplikacioneve dhe ndarjen e sigurt të informacionit personal. Kjo tematikë synon të forcojë te nxënësi kuptimin se pakujdesia në mbrojtjen e llogarive dhe të të dhënave mund të sjellë pasoja personale, shoqërore dhe financiare.

Në tematikën "Siguria në rrjetet sociale, mediat digjitale dhe verifikimi i informacionit", nxënësi analizon ndikimin që rrjetet sociale dhe mediat digjitale ushtrojnë në formimin e opinionit, në qarkullimin e përmbajtjeve dhe në drejtimin e vëmendjes së përdoruesit. Në këtë kontekst, ai zhvillon aftësi për të verifikuar burimet e informacionit, për të dalluar clickbait-in, dezinformimin, përmbajtjet e manipuluara dhe përdorimin e imazheve ose videove jashtë kontekstit. Gjithashtu, tematika trajton rolin e algoritmeve në krijimin e flluskave informuese dhe ndikimin që ato mund të kenë në mënyrën se si individi informohet, interpreton dhe ndërton qëndrime.

Në tematikën "Etika digjitale, të drejtat dhe kuadri ligjor", nxënësi reflekton mbi përgjegjësinë personale dhe mbi parimet që rregullojnë qytetarinë digjitale. Trajtohen çështje që lidhen me privatësinë, pëlqimin për publikim, të drejtën e autorit, komunikimin etik, respektin ndaj tjetrit, si dhe pasojat që sjell shpërndarja e informacionit të dëmshëm ose e përmbajtjes pa autorizim. Kjo tematikë synon të zhvillojë te nxënësi kuptimin se hapësira digjitale është pjesë e jetës shoqërore dhe publike dhe, si e tillë, kërkon sjellje të ndërgjegjshme, të përgjegjshme dhe në përputhje me normat etike dhe ligjore.

Në tematikën "Reagimi ndaj incidenteve dhe higjiena kibernetike", nxënësi mëson të veprojë në mënyrë të sigurt, të qetë dhe të strukturuar në rastet kur përballet me incidente digjitale, si kompromentimi i një llogarie, humbja e një pajisjeje, marrja e një mesazhi të

dyshimtë, përballja me bullizëm kibernetik ose dyshimi për infektim të pajisjes. Në këtë kuadër, theksi vendoset te ruajtja e provave, raportimi i incidentit, kërkimi i ndihmës dhe ndërtimi i zakoneve të qëndrueshme të higjienës kibernetike, me synim rritjen e sigurisë personale dhe parandalimin e rreziqeve në mjedisin digjital.

Përgjatë produktit final nxënësi angazhohet në punë në grup për hartimin dhe realizimin e një produkti me vlerë ndërgjegjësuese për komunitetin shkollor në fushën e sigurisë digjitale. Projekti mund të marrë forma të ndryshme, si guidë, poster, video e shkurtër, podcast, prezantim, mini-fushatë ose workshop për bashkëmoshatarët apo për nxënës më të vegjël. Përmes këtij procesi, nxënësi jo vetëm konsolidon njohuritë dhe aftësitë e fituara gjatë modulit, por i transformon ato në veprim konkret dhe në kontribut të drejtpërdrejtë për rritjen e ndërgjegjësimit dhe të kulturës së sigurisë digjitale në komunitetin shkollor.

Përmbajtja e modulit krijon mundësi për integrim ndërkurrikular me lëndë dhe fusha të ndryshme të të nxënit, duke nxitur analizën kritike, reflektimin dhe angazhimin aktiv të nxënësve të klasës së dhjetë:

Teknologjia e Informacionit dhe Komunikimit (TIK): analizimi i kërcënimeve kibernetike, vlerësimi i rreziqeve dhe zbatimi i strategjive të ndryshme për mbrojtjen e të dhënave dhe përdorimi i sigurt i teknologjisë;

Qytetaria: zhvillimi i përgjegjësisë digjitale, etikës online dhe respektit për të drejtat e të tjerëve, si dhe angazhimi aktiv në çështje që lidhen me komunitetin digjital;

Gjuha shqipe: interpretimi dhe vlerësimi kritik i përmbajtjeve digjitale, argumentimi i qëndrimeve të bazuara në fakte dhe krijimi i materialeve ndërgjegjësuese të strukturuara dhe të mirëargumentuara;

Shkencat shoqërore: analizimi i ndikimit të teknologjisë dhe mediave digjitale në shoqëri, përfshirë fenomenet e dezinformimit, manipulimit dhe ndikimit në opinionin publik;

Arte: konceptimi dhe realizimi i produkteve krijuese (posterë, video, infografikë) me mesazhe ndërgjegjësuese, duke përdorur elemente vizuale dhe komunikative të përshtatshme për audienca të ndryshme.

3. KLASA/T KU MUND TË ZHVILLOHET MODULI

Moduli mund të zhvillohet në klasën e dhjetë të arsimit të mesëm të lartë, në varësi të vendimmarrjes së shkollës. Ai ofron fleksibilitet në përshtatjen e thellësisë së përmbajtjes, të veprimtarive praktike dhe të produkteve përfundimtare, duke mundësuar që zbatimi i tij të jetë në përputhje me moshën, përvojën digjitale dhe nivelin e zhvillimit të kompetencave të

nxënësve. Ky fleksibilitet u jep mundësi shkollave ta përshtatin modulin sipas nevojave, interesave të nxënësve dhe kontekstit pedagogjik të institucionit.

4. MËSUESIT QË MUND TË ZHVILLOJNË MODULIN

Moduli rekomandohet të zhvillohet kryesisht nga mësuesit e *Teknologjisë së Informacionit dhe Komunikimit (TIK),* pasi përmbajtja dhe tematika e tij lidhen drejtpërdrejt me zhvillimin e kompetencës digjitale, përdorimin e sigurt të teknologjisë, mbrojtjen e të dhënave personale dhe qytetarinë digjitale. Megjithatë, shkolla ka *fleksibilitet* në përcaktimin e mësuesve që do ta zhvillojnë modulin, në varësi të kontekstit institucional, strukturës së stafit dhe zhvillimit profesional të tij. Në këtë kuadër, moduli mund të realizohet edhe nga mësues të tjerë të formimit ndërdisiplinor, të cilët kanë kompetencat pedagogjike dhe përgatitjen e nevojshme për të udhëhequr veprimtaritë e parashikuara. Ky fleksibilitet siguron që moduli të mos kufizohet vetëm te një fushë mësimore, por të përfitojë nga ekspertiza dhe përvoja e mësuesve në funksion të rritjes së cilësisë së procesit mësimor dhe zhvillimit të kompetencave të nxënësve.

Rekomandime për mësuesit:

Gjatë zhvillimit të modulit:

- Krijoni një mjedis të sigurt, mbështetës dhe bashkëpunues, ku nxënësit të ndihen të lirshëm për të diskutuar përvoja, shqetësime dhe dilema që lidhen me përdorimin e teknologjisë dhe të internetit.
- Përdorni gjuhë të qartë dhe të saktë, duke shpjeguar termat teknikë në mënyrë të kuptueshme dhe të lidhur me situata reale nga jeta e përditshme e nxënësve.
- Nxitni të menduarit kritik, analizën dhe reflektimin, duke i udhëhequr nxënësit të mos mjaftohen vetëm me identifikimin e rrezikut, por edhe me kuptimin e shkaqeve, pasojave dhe mënyrave të reagimit.
- Përdorni shembuj, raste studimore dhe situata të afërta me realitetin e nxënësve, në mënyrë që përmbajtja e modulit të jetë sa më konkrete, domethënëse dhe e zbatueshme.
- Theksoni në mënyrë të vazhdueshme lidhjen ndërmjet sigurisë kibernetike, qytetarisë digjitale, etikës së komunikimit dhe përgjegjësisë personale në mjedisin online.
- Inkurajoni diskutime të hapura dhe të argumentuara mbi çështje si privatësia, reputacioni digjital, dezinformimi, manipulimi i informacionit, bullizmi kibernetik dhe të drejtat në mjedisin digjital.

- Fokusohuni jo vetëm te rreziqet, por edhe te masat praktike të mbrojtjes, te mënyrat e verifikimit dhe te hapat konkretë të reagimit në situata problematike.
- Jepni komente vlerësuese dhe udhëzuese gjatë gjithë procesit, duke mbështetur zhvillimin e aftësive praktike, të qëndrimeve etike dhe të përgjegjësisë digjitale te nxënësit.

Menaxhimi i situatave të ndjeshme

- Tregoni kujdes dhe ndjeshmëri gjatë trajtimit të çështjeve që mund të lidhen me përvoja personale të nxënësve, si bullizmi kibernetik, cenimi i privatësisë, mashtrimet online ose përmbajtjet shqetësuese.
- Shmangni trajtimin sensacional, alarmues ose frikësues të rasteve dhe orientoni diskutimin drejt mbështetjes, parandalimit dhe zgjidhjes.
- Inkurajoni nxënësit të kërkojnë ndihmë dhe të raportojnë situatat problematike te një i rritur i besuar, te shkolla ose te strukturat përkatëse mbështetëse.
- Respektoni privatësinë e nxënësve gjatë diskutimeve dhe shmangni ekspozimin e rasteve personale në mënyrë të drejtpërdrejtë ose identifikuese.
- Në rastet kur evidentohen shqetësime konkrete, bashkëpunoni me prindërit, psikologun e shkollës dhe strukturat e tjera mbështetëse, sipas nevojës.

Përshtatja e modulit

- Përshtatini veprimtaritë sipas nivelit të njohurive, përvojës digjitale dhe nevojave konkrete të nxënësve të klasës.
- Thelloni ose thjeshtoni trajtimin e çështjeve të caktuara në varësi të interesit të nxënësve dhe kontekstit të shkollës.
- Përzgjidhni dhe përshtatni raste studimore, skenarë dhe materiale që lidhen me realitetin e përditshëm të adoleshentëve dhe me platformat që ata përdorin më shpesh.
- Shfrytëzoni mundësitë për integrim ndërkurrikular, sidomos me qytetarinë, gjuhën shqipe dhe fusha të tjera që lidhen me analizën kritike, etikën dhe komunikimin.
- Mund të planifikoni, sipas mundësive dhe në bashkëpunim me drejtuesit e shkollës, përfshirjen e ekspertëve nga fusha e sigurisë kibernetike, medias, psikologjisë ose institucioneve mbështetëse, të cilët mund të kontribuojnë me njohuri dhe përvoja praktike.

5. KOHËZGJATJA E MODULIT

Moduli mund të integrohet në kurrikulën me bazë shkolle ose në kurrikulën me zgjedhje si një program i plotë prej **36 orësh** mësimore. Ai mund të zbatohet duke përfshirë veprimtaritë e sugjeruara për secilën tematikë, si dhe veprimtari të tjera që mësuesi i vlerëson të përshtatshme, në përputhje me nevojat dhe kontekstin e nxënësve.

Nr.	Tematika	Orët mësimore të sugjeruara[1]
1	Ekosistemi digjital, identiteti online dhe gjurma digjitale	4 orë
2	Kërcënimet kibernetike dhe llojet e sulmeve	6 orë
3	Mbrojtja e llogarive, fjalëkalimeve dhe të dhënave personale	6 orë
4	Siguria në rrjetet sociale, mediat digjitale dhe verifikimi i informacionit	5 orë
5	Etika digjitale, të drejtat dhe kuadri ligjor	4 orë
6	Reagimi ndaj incidenteve dhe higjiena kibernetike	5 orë
7	Projekt final dhe ndërgjegjësim në komunitet	6 orë

6. REZULTATET E TË NXËNIT

Rezultatet e të nxënit
Ekosistemi digjital, identiteti online dhe gjurma digjitale
Nxënësi: • analizon identitetin online, reputacionin digjital dhe gjurmën digjitale aktive dhe pasive në funksion të pranisë së individit në mjedisin digjital; • përshkruan të dhënat personale, të dhënat sensitive dhe informacionin që mund të ndahet në mënyrë publike; • vlerëson ndikimin që postimet, komentet, fotografitë dhe ndërveprimet online kanë në perceptimin e të tjerëve dhe në reputacionin personal; • analizon rreziqet që lidhen me ndarjen e tepruar ose të pakujdesshme të informacionit personal; • zbaton parime të sigurisë dhe të përgjegjësisë në menaxhimin e profileve personale dhe pranisë së vet digjitale; • harton rregulla personale për menaxhimin e sigurt dhe etik të identitetit të vet online.

[1] *Orët e sugjeruara për tematika janë orientuese dhe mund të përshtaten nga mësuesit, të cilët kanë fleksibilitetin të riorganizojnë kohën dhe veprimtaritë sipas nevojave të nxënësve dhe kontekstit të klasës.*

Kërcënimet kibernetike dhe llojet e sulmeve
Nxënësi: • identifikon format më të zakonshme të kërcënimeve kibernetike që shfaqen në mjedisin digjital, si phishing-u, malware-i, profilet e rreme, mashtrimet me oferta, manipulimi social dhe bullizmi kibernetik; • analizon shenjat paralajmëruese të mesazheve, lidhjeve, profileve ose skedarëve të dyshimtë; • shpjegon mënyrat se si përdoren urgjenca, frika, kurioziteti ose shpërblimi për të manipuluar përdoruesin; • analizon skenarë të cenimit të sigurisë së një individi, grupi ose komuniteti shkollor; • përdor terminologjinë bazë të sigurisë kibernetike në mënyrë të saktë dhe funksionale; • propozon masa parandaluese për zvogëlimin e rrezikut në situata të zakonshme online.
Mbrojtja e llogarive, fjalëkalimeve dhe të dhënave personale
Nxënësi: • krijon fjalëkalime ose passphrase të forta, duke shmangur zgjedhjet e parashikueshme; • shpjegon rëndësinë e përdorimit të fjalëkalimeve të ndryshme për llogari të ndryshme; • shpjegon funksionin e autentikimit me dy faktorë në mbrojtjen e llogarive; • vlerëson lejet e aplikacioneve në funksion të privatësisë dhe sigurisë personale; • zbaton praktika të sigurta për përditësimin e pajisjeve, rezervimin e të dhënave dhe ruajtjen e skedarëve; • harton një listë kontrolli personale për mbrojtjen e llogarive, pajisjeve dhe të dhënave personale.
Siguria në rrjetet sociale, mediat digjitale dhe verifikimi i informacionit
Nxënësi: • vlerëson besueshmërinë e burimeve të informacionit në mjedisin digjital; • identifikon lajmet e rreme, clickbait-in, manipulimin emocional, përmbajtjen e manipuluar dhe informacionin e nxjerrë jashtë kontekstit; • analizon ndikimin e algoritmeve në përzgjedhjen dhe shpërndarjen e informacionit; • zbaton hapa të strukturuar për verifikimin e informacionit përpara se ta besojë ose ta shpërndajë; • demonstron qëndrim kritik dhe të përgjegjshëm në përdorimin e rrjeteve sociale dhe mediave digjitale.
Etika digjitale, të drejtat dhe kuadri ligjor

Nxënësi:

- analizon kuptimin e qytetarisë digjitale në lidhje me të drejtat dhe përgjegjësitë e përdoruesit;
- dallon sjelljet e papërshtatshme online nga veprimet që cenojnë privatësinë, dinjitetin ose të drejtat e të tjerëve;
- zbaton parimet e pëlqimit, privatësisë, të drejtës së autorit dhe komunikimit etik në situata të ndryshme digjitale;
- analizon raste që lidhen me bullizmin kibernetik, shpërndarjen pa leje të përmbajtjes ose përdorimin e paautorizuar të të dhënave;
- argumenton qëndrime në dilema etike dhe juridike që lidhen me përdorimin e teknologjisë.

Reagimi ndaj incidenteve dhe higjiena kibernetike

Nxënësi:

- identifikon situata që përbëjnë incident digjital ose rrezik të menjëhershëm për sigurinë personale;
- përshkruan hapat bazë të reagimit ndaj incidenteve digjitale;
- dallon veprimet që duhen ndërmarrë dhe ato që duhen shmangur kur llogaria, pajisja ose reputacioni online rrezikohet;
- vlerëson rolin e mësuesit, prindit, shkollës dhe platformës digjitale në procesin e raportimit dhe mbështetjes;
- harton një plan të thjeshtë personal për reagim ndaj incidenteve digjitale.

Projekt final dhe ndërgjegjësim në komunitet

Nxënësi:

- përzgjedh një temë me interes për komunitetin shkollor në fushën e sigurisë kibernetike dhe qytetarisë digjitale;
- bashkëpunon në grup për planifikimin, organizimin dhe realizimin e një produkti final;
- krijon materiale ndërgjegjësuese të kuptueshme, të sakta dhe të përshtatshme për audiencën e synuar;
- prezanton gjetjet, mesazhet dhe rekomandimet në mënyrë të qartë dhe të strukturuar;
- reflekton mbi procesin e punës, kontributin personal dhe zbatueshmërinë e njohurive të fituara në jetën reale.

7. VEPRIMTARITË PRAKTIKE

Në vijim paraqiten veprimtari praktike të sugjeruara, të organizuara sipas tematikave të modulit. Këto veprimtari synojnë të mbështesin zhvillimin e njohurive, aftësive dhe qëndrimeve të nxënësve në fushën e sigurisë kibernetike. Mësuesi mund t'i përzgjedhë, t'i përshtatë ose t'i plotësojë ato në varësi të nevojave të klasës, kohës në dispozicion dhe kontekstit të shkollës, duke ruajtur lidhjen me tematikat dhe rezultatet e të nxënit të modulit.

EKOSISTEMI DIGJITAL, IDENTITETI ONLINE DHE GJURMA DIGJITALE

Veprimtari: Gjurma digjitale dhe pasojat e saj

Qëllimi i veprimtarisë: Nxënësit analizojnë mënyrën se si ndërtohet gjurma digjitale dhe vlerësojnë pasojat që ajo mund të ketë në privatësi, reputacion dhe mundësi personale e profesionale.

Përshkrimi i veprimtarisë: Mësuesi e nis veprimtarinë me një pyetje problemore: *"A është interneti një hapësirë ku gjërat harrohen shpejt, apo një hapësirë ku gjithçka mund të mbetet?"* Mbi këtë pyetje zhvillohet një diskutim i shkurtër hyrës, ku nxënësit reflektojnë mbi përvojat e tyre dhe mbi mënyrën si krijohen gjurmët digjitale. Në vijim, mësuesi prezanton shkurt dallimin ndërmjet gjurmës digjitale aktive dhe asaj pasive, duke e lidhur me shembuj konkretë nga përdorimi i përditshëm i teknologjisë: postime, komente, kërkime, regjistrime në platforma, përdorim aplikacionesh, vendndodhje, cookies, historik klikimesh etj.

Më pas, nxënësit punojnë në grupe dhe analizojnë disa situata të përgatitura nga mësuesi, si p.sh.:

- një koment i shkruar me nxitim në një rrjet social;
- publikimi i një fotografie pa menduar për audiencën;
- regjistrimi në një platformë me të dhëna të panevojshme;
- përdorimi i një aplikacioni që mbledh shumë të dhëna personale;
- shpërndarja e një përmbajtjeje që më vonë hiqet, por mbetet e ruajtur diku tjetër.

Për secilin rast, nxënësit diskutojnë:

- Çfarë gjurme lë ky veprim?
- Kush mund ta përdorë ose ta shohë këtë informacion?
- Cilat mund të jenë pasojat afatshkurtra dhe afatgjata?
- Si mund të shmangej ose të reduktohej kjo gjurmë?

Në vijim, secili grup ndërton një skemë analitike ku lidh: ***veprimin digjital → gjurmën e lënë → pasojën e mundshme → masën parandaluese.***

Në fund, zhvillohet një reflektim i përbashkët mbi faktin se gjurma digjitale nuk ndikon vetëm në sigurinë personale, por edhe në mënyrën si ndërtohet identiteti dhe reputacioni i individit në mjedisin digjital.

Produkti i mundshëm:

- Skemë analitike e gjurmës digjitale dhe pasojave të saj;
- Reflektim individual: *"Si mund ta menaxhoj më me kujdes gjurmën time digjitale?"*

Veprimtari: Auditimi i pranisë digjitale

***Qëllimi i veprimtarisë*:** Nxënësit analizojnë një profil digjital të simuluar, identifikojnë elementet që mund të ndikojnë në privatësi dhe reputacion, si dhe propozojnë mënyra për ta bërë atë më të sigurt dhe më të përshtatshëm.

Përshkrimi i veprimtarisë: Veprimtaria nis me një pyetje hyrëse nga mësuesi: **"***Çfarë mund të kuptojë dikush për një person vetëm duke parë profilin e tij online?"* Përmes një diskutimi të shkurtër, nxënësit rikujtojnë se prania digjitale ndërtohet nga postimet, komentet, fotografitë, pëlqimet, ndjekësit, gjuha e përdorur dhe mënyra si menaxhohen cilësimet e privatësisë.

Më pas, mësuesi paraqet një profil digjital të simuluar, të ndërtuar posaçërisht për këtë veprimtari. Profili mund të përfshijë:

- fotografi profili dhe përshkrim personal;
- disa postime publike;
- komente ose reagime ndaj postimeve;
- lista interesash;
- informacione personale të dukshme;
- cilësime privatësie.

Në vijim, nxënësit ndahen në grupe dhe punojnë me një **fletë auditimi**, ku analizojnë profilin sipas disa treguesve të qartë. Për secilin element, ata përcaktojnë:

- çfarë informacioni jep ai për personin;
- nëse përbën rrezik për privatësinë;
- nëse mund të ndikojë në reputacionin digjital;
- çfarë do të duhej ndryshuar.

Për ta bërë analizën më të strukturuar, grupet mund të përdorin një vlerësim të thjeshtë:

- ✓ rrezik i ulët,
- ✓ rrezik mesatar,
- ✓ rrezik i lartë.

Pas analizës, secili grup përzgjedh:

- 3 elementet më problematike të profilit;
- 3 rekomandime konkrete për përmirësim.

Më pas, grupet prezantojnë gjetjet e tyre para klasës. Mësuesi udhëheq diskutimin duke i ndihmuar nxënësit të kuptojnë se prania digjitale nuk ndikon vetëm në mënyrën si paraqitemi online, por edhe në reputacionin, marrëdhëniet dhe mundësitë tona në të ardhmen.

Në përfundim, secili nxënës plotëson individualisht një reflektim të shkurtër me pyetjen: *"Çfarë duhet të kem parasysh për ta menaxhuar më me kujdes praninë time digjitale?"*

Produkti i mundshëm:

- Fletë auditimi e profilit digjital;
- Listë me 3 problemet kryesore dhe 3 rekomandime për përmirësim;
- Reflektim individual mbi menaxhimin e pranisë digjitale.

Veprimtari: Reputacioni digjital në të ardhmen

***Qëllimi i veprimtarisë*:** Nxënësit vlerësojnë ndikimin që prania dhe sjellja digjitale mund të kenë në mundësitë e tyre akademike, profesionale dhe shoqërore në të ardhmen.

Përshkrimi i veprimtarisë: Veprimtaria nis me një pyetje nga mësuesi: **"***A mund të ndikojë ajo që postojmë sot në mundësitë tona nesër?"* Nxënësit japin mendime dhe ndajnë shembuj nga përvoja e tyre ose nga raste që kanë dëgjuar.

Më pas, mësuesi paraqet 2–3 skenarë të shkurtër, si p.sh.:

- një nxënës që aplikon për bursë ose shkëmbim studentor dhe profili i tij publik përmban gjuhë fyese ose postime të papërshtatshme;
- një i ri që kërkon një punë të parë dhe ka lënë online komente diskriminuese ose tallëse;
- një nxënës që ka ndërtuar një profil digjital pozitiv përmes përmbajtjeve krijuese, aktiviteteve dhe komunikimit të përgjegjshëm.

Në grupe, nxënësit analizojnë secilin rast dhe diskutojnë:

- Çfarë përshtypjeje krijon ky profil?
- Cilat elemente ndikojnë pozitivisht ose negativisht?
- Si mund të ndryshojë reputacioni digjital mundësitë e këtij personi?
- Çfarë do të rekomandonin për ta përmirësuar praninë e tij digjitale?

Në vijim, grupet prezantojnë përfundimet e tyre dhe mësuesi thekson se reputacioni digjital nuk lidhet vetëm me rrezikun, por edhe me mënyrën si ndërtojmë besueshmëri, seriozitet dhe identitet në mjedisin online.

Në fund, secili nxënës shkruan një reflektim të shkurtër me temë: *"Si dua të duket prania ime digjitale pas 5 vitesh?"*

Produkti i mundshëm:

- Analizë e shkurtër e një skenari;
- Reflektim individual mbi reputacionin digjital në të ardhmen.

KËRCËNIMET KIBERNETIKE DHE LLOJET E SULMEVE

Veprimtari: Detektivët e phishing-ut

***Qëllimi i veprimtarisë*:** Nxënësit analizojnë mesazhe dhe email-e të ndryshme për të identifikuar shenjat paralajmëruese të phishing-ut dhe për të dalluar komunikimin e besueshëm nga ai mashtrues.

***Përshkrimi i veprimtarisë*:** Veprimtaria nis me paraqitjen nga mësuesi të disa shembujve të printuar ose të projektuar të mesazheve dhe email-eve, ku disa janë legjitime dhe disa të tjera përmbajnë elemente tipike të phishing-ut. Fillimisht, nxënësit i vëzhgojnë rastet individualisht dhe shënojnë elementet që u duken të dyshimta.

Më pas, nxënësit punojnë në grupe dhe përdorin një fletë analize për të vlerësuar secilin shembull sipas disa treguesve, si:

- adresa e dërguesit;
- toni urgjent ose kërcënues;
- gabimet gjuhësore;
- kërkesa për klikim të menjëhershëm;
- kërkesa për ndarjen e të dhënave personale;
- lidhje ose bashkëngjitje të dyshimta.

Për secilin rast, grupet vendosin nëse mesazhi është:

- ✓ i besueshëm;
- ✓ i dyshimtë;
- ✓ i rrezikshëm,

dhe argumentojnë vendimin e tyre. Në vijim, grupet prezantojnë analizën para klasës dhe mësuesi përmbledh në tabelë shenjat më të zakonshme paralajmëruese të phishing-ut.

Për ta forcuar veprimtarinë, mësuesi mund të shtojë edhe një hap krahasues, ku nxënësit analizojnë dallimin ndërmjet:

- adresës reale dhe adresës së manipuluar të një domeni;
- lidhjeve të plota dhe lidhjeve të shkurtuara;
- gjuhës zyrtare dhe gjuhës manipuluese në komunikimin digjital.

Produkti i mundshëm:

- Tabelë klasifikimi e rasteve;
- Listë ose poster me titull: **"***Shenjat paralajmëruese të një mesazhi phishing."*

Veprimtari: Loja me role "Manipulimi social"

Qëllimi i veprimtarisë: Nxënësit analizojnë mekanizmat e manipulimit social dhe vlerësojnë mënyrat e reagimit të sigurt ndaj situatave që synojnë marrjen e informacionit ose cenimin e sigurisë personale.

Përshkrimi i veprimtarisë: Mësuesi e nis veprimtarinë duke shpjeguar shkurt se shumë sulme digjitale nuk mbështeten vetëm te mjetet teknike, por edhe te manipulimi i përdoruesit përmes emocioneve, besimit, nxitimit ose frikës.

Më pas, nxënësit ndahen në grupe dhe secilit grup i jepet një skenar i ndryshëm, si p.sh.:

- një person që prezantohet si administrator platforme;
- një shok i rremë që kërkon kod verifikimi;
- një konkurs fitues që kërkon të dhëna personale;
- një mesazh që nxit frikë për të marrë informacion;
- një telefonatë ose komunikim që kërkon veprim të menjëhershëm.

Grupet analizojnë skenarin duke iu përgjigjur pyetjeve:

- Cilat emocione ose reagime synon të nxisë ky komunikim?
- Cili është rreziku kryesor?
- Çfarë elementi e bën mesazhin bindës?
- Si duhet të reagojë një nxënës në mënyrë të sigurt dhe të arsyetuar?

Në vijim, grupet paraqesin skenarin dhe zgjidhjen përpara klasës. Mësuesi e orienton diskutimin drejt kuptimit se manipulimi social funksionon pikërisht sepse shfrytëzon dobësi njerëzore, si besimi, kureshtja, frika ose nxitimi. Mësuesi mund t'u kërkojë nxënësve të identifikojnë për secilin rast teknikën e manipulimit të përdorur, objektivin e sulmit, si dhe masën parandaluese më efektive.

Produkti i mundshëm:

- Kartë-zgjidhje për skenarin e analizuar;
- Fjalor i shkurtër me taktikat më të zakonshme të manipulimit social.

Veprimtari: Klasifikimi i kërcënimeve në jetën e përditshme

Qëllimi i veprimtarisë: Nxënësit klasifikojnë kërcënime të ndryshme digjitale sipas natyrës së tyre dhe propozojnë masa parandaluese në situata të afërta me jetën e përditshme të adoleshentëve.

Përshkrimi i veprimtarisë: Mësuesi paraqet një seri rastesh të shkurtra që lidhen me përvojat digjitale të përditshme të të rinjve, si:

- lidhje të dyshimta në chat;
- lojëra ose aplikacione që kërkojnë leje të tepërta;
- profile të rreme në rrjetet sociale;
- mesazhe bullizuese;
- skedarë të paautorizuar të dërguar me email;
- reklama mashtruese ose oferta joshëse;
- kërkesa të papritura për kod verifikimi ose të dhëna hyrjeje.

Nxënësit punojnë në grupe dhe i rendisin rastet sipas llojit të kërcënimit, p.sh.:

- rrezik teknik;
- rrezik social;
- rrezik emocional;
- rrezik për privatësinë;
- rrezik për reputacionin.

Për secilin rast, ata propozojnë edhe masat parandaluese që mund të ndihmojnë në shmangien ose zvogëlimin e rrezikut. Grupet prezantojnë skemat e tyre dhe i krahasojnë me ato të grupeve të tjera.

Në përfundim, mësuesi përmbledh idenë se kërcënimet digjitale nuk paraqiten gjithmonë në të njëjtën formë dhe se përdoruesi duhet të zhvillojë aftësinë për t'i njohur, klasifikuar dhe trajtuar ato në mënyrë të vetëdijshme.

Produkti i mundshëm:

- Skemë klasifikuese e kërcënimeve;
- Listë e masave parandaluese për secilin rast.

Veprimtari: Analiza e filmit interaktiv "No Escape Room"

Qëllimi i veprimtarisë: Nxënësit analizojnë mekanizmat e manipulimit dhe të presionit që përdoren në mjedisin digjital, si dhe reflektojnë mbi mënyrat e reagimit të sigurt dhe të përgjegjshëm në situata të rrezikshme online.

Përshkrimi i veprimtarisë: Veprimtaria zhvillohet mbi bazën e filmit interaktiv **"No Escape Room"**, një burim edukativ online që paraqet, në formë të ndërveprueshme, mënyrën se si një i ri mund të manipulohet dhe të përfshihet në një situatë shantazhi ose sextortion-i në internet. Mësuesi e prezanton shkurt burimin dhe orienton nxënësit të vëzhgojnë me kujdes mënyrën se

si ndërtohet besimi, si përdoren profilet e rreme, si krijohet presioni psikologjik dhe si përshkallëzohet situata.

Pas ndjekjes së materialit, nxënësit punojnë në grupe dhe diskutojnë pyetje të tilla si:

- Cilat taktika manipulimi u përdorën në këtë rast?
- Cilat ishin shenjat paralajmëruese që personazhi mund të kishte dalluar më herët?
- Në cilat momente situata mund të ishte ndalur?
- Çfarë duhet të bëjë një i ri kur përballet me një situatë të ngjashme?
- Cili është roli i raportimit dhe i kërkimit të ndihmës?

Në vijim, grupet prezantojnë përfundimet e tyre dhe mësuesi e lidh diskutimin me tema më të gjera të sigurisë kibernetike, si manipulimi social, profilet e rreme, privatësia, shantazhi digjital dhe reagimi ndaj incidenteve.

Produkti i mundshëm:

- Listë me shenjat paralajmëruese dhe hapat e reagimit në situata manipulimi online;
- Reflektim individual me temë: ***"Çfarë duhet të kem parasysh për të mbrojtur veten në komunikimin online?"***

Nëse do ta përmendësh si burim konkret në dokument, mund të vendosësh thjesht: **Burim i sugjeruar:** No Escape Room (NCMEC) https://noescaperoom.org/

Për shkak se materiali trajton një çështje të ndjeshme, rekomandohet që përdorimi i tij të shoqërohet me orientim pedagogjik të kujdesshëm dhe me diskutim të strukturuar në klasë, në mënyrë që nxënësit ta përpunojnë përmbajtjen në mënyrë të sigurt dhe reflektuese.

MBROJTJA E LLOGARIVE, FJALËKALIMEVE DHE TË DHËNAVE PERSONALE

Veprimtari: Laboratori i fjalëkalimeve të forta

Qëllimi i veprimtarisë: Nxënësit vlerësojnë sigurinë e fjalëkalimeve të ndryshme dhe kuptojnë kriteret që e bëjnë një fjalëkalim të fortë, të qëndrueshëm dhe të vështirë për t'u hamendësuar.

Përshkrimi i veprimtarisë: Mësuesi nis veprimtarinë duke paraqitur në tabelë ose me projektor disa shembuj fjalëkalimesh të ndryshme, pa përdorur asnjë të dhënë reale të nxënësve. Shembujt mund të përfshijnë raste shumë të dobëta, mesatare dhe më të forta. Nxënësit, fillimisht individualisht, i rendisin ato nga më i dobëti te më i sigurti dhe japin shkurt arsyetimin e tyre.

Më pas, puna vazhdon në çifte ose grupe të vogla. Secili grup analizon shembujt duke u mbështetur në disa tregues të qartë:

- gjatësia e fjalëkalimit;

- përdorimi i shkronjave të mëdha dhe të vogla;
- përdorimi i numrave dhe simboleve;
- shmangia e emrave, datëlindjeve dhe fjalëve të zakonshme;
- mundësia e ripërdorimit në llogari të tjera.

Në vijim, mësuesi përmbledh kriteret kryesore të një fjalëkalimi të sigurt dhe prezanton shkurt edhe idenë e passphrase, si një mënyrë më e sigurt dhe më e lehtë për t'u mbajtur mend. Pas kësaj, nxënësit krijojnë modele fjalëkalimesh ose passphrase-sh sipas rregullave të mësuara, pa përdorur informacion personal real. Në fund, zhvillohet një diskutim i shkurtër mbi pyetjen: "*Pse një fjalëkalim i fortë nuk mjafton gjithmonë, nëse përdoret njësoj në shumë llogari?"* Kjo ndihmon mësuesin ta lidhë veprimtarinë me menaxhimin më të gjerë të sigurisë së llogarive.

Produkti i mundshëm:

- Listë me fjalëkalime të sugjeruara nga platforma (password gjenerator)
- Listë me rregulla për krijimin e fjalëkalimeve të sigurta.

Veprimtari: Klinika e privatësisë dhe lejeve të aplikacioneve

Qëllimi i veprimtarisë: Nxënësit analizojnë lejet që kërkojnë aplikacionet dhe vlerësojnë ndikimin e tyre në privatësi, siguri dhe mbrojtjen e të dhënave personale.

Përshkrimi i veprimtarisë: Mësuesi paraqet disa shembuj aplikacionesh ose përshkrime të thjeshtuara të tyre, ku shfaqen leje të ndryshme, si qasje në kamerë, mikrofon, kontakte, vendndodhje, galeri ose skedarë. Fillimisht, klasa diskuton pyetjen: "A ka gjithmonë nevojë reale një aplikacion për të gjitha lejet që kërkon?" Më pas, nxënësit ndahen në grupe dhe secilit grup i jepen 2–3 raste konkrete aplikacionesh. Ata analizojnë për secilin rast:

- cilat leje janë të nevojshme për funksionin e aplikacionit;
- cilat leje kërkojnë kujdes;
- cilat duken të panevojshme ose të tepërta;
- çfarë rreziku mund të krijojë pranimi i tyre.

Për ta bërë punën më të qartë, grupet plotësojnë një tabelë me tre kolona:

- ✓ Leje e domosdoshme
- ✓ Leje që kërkon kujdes
- ✓ Leje e panevojshme

Në vijim, grupet prezantojnë përfundimet dhe argumentojnë pse një leje duhet pranuar ose jo. Mësuesi e përmbyll diskutimin duke theksuar se mbrojtja e të dhënave personale nuk lidhet vetëm me atë që publikojmë, por edhe me atë që autorizojmë pa e vlerësuar mjaftueshëm.

Në fund, secili grup harton një listë të shkurtër me pyetje që duhet t'ia bëjë vetes çdo përdorues përpara instalimit ose përdorimit të një aplikacioni.

Produkti i mundshëm:

- Tabelë vlerësimi e lejeve të aplikacioneve;
- Rekomandime për përdorim më të sigurt të aplikacioneve.

Veprimtari: Rezervimi i të dhënave dhe lista e higjienës digjitale

***Qëllimi i veprimtarisë*:** Nxënësit analizojnë situata të humbjes së aksesit ose të të dhënave dhe ndërmarrin hapa konkretë për mbrojtjen, rikuperimin dhe reagimin e sigurt.

Përshkrimi i veprimtarisë: Veprimtaria nis me një situatë-problem të paraqitur nga mësuesi: *"Telefoni yt humbet, llogaria jote bllokohet ose kompjuteri yt nuk ndizet më. Çfarë humbet fillimisht dhe çfarë bën më pas?"* Nxënësit japin përgjigje të shpejta dhe mësuesi i përmbledh në tabelë, duke evidentuar llojet e të dhënave që zakonisht rrezikohen, si kontaktet, fotografitë, dokumentet, materialet shkollore, llogaritë e lidhura dhe informacionet personale.

Më pas, klasa ndahet në grupe dhe secilit grup i jepet një skenar i ndryshëm, si p.sh.:

- humbja e telefonit;
- bllokimi ose kompromentimi i email-it;
- dëmtimi i pajisjes ku ruhen materialet shkollore;
- humbja e aksesit në një llogari për shkak të mungesës së të dhënave të rikuperimit.

Çdo grup punon me një **fletë-zgjidhje**, ku duhet të analizojë rastin sipas katër pyetjeve kryesore:

- Çfarë rrezikohet të humbet?
- Çfarë duhej bërë më parë për ta parandaluar situatën?
- Cilat hapa duhen ndërmarrë menjëherë?
- Cilat masa duhen marrë më pas për të rikuperuar ose mbrojtur llogarinë dhe të dhënat?

Për ta bërë veprimtarinë më interaktive, mësuesi mund ta organizojë si sfidë në kohë: secili grup ka disa minuta për të ndërtuar planin e reagimit dhe më pas e prezanton atë para klasës. Gjatë prezantimit, grupet e tjera mund të shtojnë një hap që mungon ose të propozojnë një zgjidhje më të mirë.

Në vijim, mësuesi përmbledh veprimet kryesore që ndihmojnë në parandalim dhe rikuperim, si:

- rezervimi i të dhënave;
- përdorimi i të dhënave të rikuperimit;
- përditësimi i pajisjeve;

- aktivizimi i bllokimit dhe lokalizimit të pajisjes;
- organizimi i sigurt i skedarëve të rëndësishëm.

Në fund, secili nxënës harton një **mini-plan personal të reagimit**, ku përcakton çfarë do të bënte në rast humbjeje të pajisjes, bllokimi të llogarisë ose humbjeje të të dhënave, si dhe cilat masa parandaluese do të zbatojë për të ulur rrezikun.

Produkti i mundshëm:

- Skemë reagimi për një nga skenarët e dhënë;
- Mini-plan personal për mbrojtjen dhe rikuperimin e llogarive dhe të të dhënave.

SIGURIA NË RRJETET SOCIALE, MEDIAT DIGJITALE DHE VERIFIKIMI I INFORMACIONIT

Veprimtari: Laboratori i verifikimit të informacionit

Qëllimi i veprimtarisë: Nxënësit zbatojnë hapa konkretë për verifikimin e informacionit dhe vlerësojnë besueshmërinë e përmbajtjeve që qarkullojnë në rrjetet sociale dhe mediat digjitale.

Përshkrimi i veprimtarisë*:** Veprimtaria nis me paraqitjen nga mësuesi të disa lajmeve, postimeve, titujve ose fotografive që janë shpërndarë gjerësisht në rrjetet sociale. Mësuesi i fton nxënësit të reflektojnë fillimisht mbi pyetjen: **"Çfarë na bën ta besojmë menjëherë një informacion që shohim online?"*

Më pas, nxënësit ndahen në grupe dhe secili grup merr një material për analizë. Duke përdorur një fletë pune, ata verifikojnë:

- kush e ka publikuar informacionin;
- kur është publikuar;
- nëse ka autor ose institucion të identifikueshëm;
- nëse përmenden burime të mbështetura;
- nëse i njëjti informacion konfirmohet nga burime të tjera;
- nëse titulli përputhet me përmbajtjen;
- nëse materiali mund të jetë nxjerrë jashtë kontekstit.

Në vijim, grupet prezantojnë përfundimet e tyre dhe argumentojnë nëse materiali është:

- i besueshëm;
- i dyshimtë;
- ose i pabesueshëm.

Mësuesi përmbyll veprimtarinë duke theksuar se besueshmëria e një informacioni nuk matet nga numri i pëlqimeve, komenteve apo shpërndarjeve, por nga cilësia e burimit, qartësia e autorësisë dhe forca e provave.

Produkti i mundshëm:

- Fletë pune me hapat e verifikimit;
- Përmbledhje grupi me titull: *"Si ta kontrollojmë një informacion para se ta shpërndajmë?"*

Veprimtari: Algoritmet dhe flluska informuese

Qëllimi i veprimtarisë: Nxënësit analizojnë ndikimin e algoritmeve në përzgjedhjen e përmbajtjes që u shfaqet dhe reflektojnë mbi mënyrën se si kjo ndikon në formimin e opinionit.

Përshkrimi i veprimtarisë: Mësuesi e nis veprimtarinë me një pyetje të thjeshtë: **"***Pse dy persona që përdorin të njëjtën platformë nuk shohin domosdoshmërisht të njëjtën përmbajtje?"*

Mbi këtë pyetje zhvillohet një diskutim hyrës, ku nxënësit ndajnë përvoja nga përdorimi i rrjeteve sociale, motorëve të kërkimit ose platformave video/audio.

Në vijim, mësuesi shpjegon në mënyrë të thjeshtë se algoritmet e platformave digjitale priren t'u shfaqin përdoruesve përmbajtje të ngjashme me atë që kanë pëlqyer, klikuar ose kërkuar më parë. Për ta konkretizuar, nxënësit analizojnë disa skenarë të shkurtër përdoruesish me interesa të ndryshme dhe diskutojnë se çfarë lloj përmbajtjeje ka më shumë gjasa t'u shfaqet secilit.

Më pas, nxënësit punojnë në grupe dhe diskutojnë:

- si ndikon kjo në mënyrën si informohemi;
- si mund të krijohen "flluska informuese";
- çfarë rreziku sjell ekspozimi i kufizuar ndaj këndvështrimeve të ndryshme;

Në përfundim, klasa harton një listë me strategji që ndihmojnë në zgjerimin e burimeve të informacionit, si ndjekja e burimeve të ndryshme, krahasimi i këndvështrimeve dhe verifikimi i informacionit përpara se të besohet ose të shpërndahet.

Produkti i mundshëm:

- Hartë idesh mbi ndikimin e algoritmeve në informacion;
- Listë strategjish për diversifikimin e burimeve dhe shmangien e flluskës informuese.

Veprimtari: Analiza e përmbajtjes së manipuluar

***Qëllimi i veprimtarisë*:** Nxënësit identifikojnë shenja që mund të tregojnë manipulim të përmbajtjes digjitale dhe zhvillojnë vigjilencë kritike ndaj imazheve, videove dhe materialeve të shpërndara online.

***Përshkrimi i veprimtarisë*:** Veprimtaria nis me paraqitjen nga mësuesi të disa shembujve ilustrues të imazheve, videove ose postimeve që mund të jenë manipuluar ose nxjerrë jashtë kontekstit. Mësuesi orienton nxënësit të mos fokusohen vetëm te përmbajtja, por te elementet që ngrenë dyshime për besueshmërinë e saj.

Në grupe, nxënësit analizojnë materialet duke përdorur një fletë vëzhgimi, ku kontrollojnë:

- nëse materiali ka burim të qartë;
- nëse titulli është i ekzagjeruar ose emocional;
- nëse ka mungesë të kontekstit për kohën dhe vendin;
- nëse cilësia vizuale është e pazakontë;
- nëse materiali është shkëputur nga një përmbajtje më e gjerë;
- nëse mesazhi përpiqet të nxisë reagim të menjëhershëm emocional.

Në vijim, secili grup prezanton gjetjet dhe argumenton pse materiali i analizuar është i besueshëm, i dyshimtë ose potencialisht i manipuluar. Mësuesi përmbyll duke theksuar se jo çdo material i dyshimtë është domosdoshmërisht i rremë, por çdo material i dyshimtë kërkon verifikim të mëtejshëm.

Për ta bërë më interesante, mësuesi mund ta organizojë veprimtarinë si një **sfidë klasore**, ku grupet duhet të justifikojnë me prova pse një material duhet trajtuar me kujdes.

Produkti i mundshëm:

- Fletë vëzhgimi e shenjave paralajmëruese;
- Mini-udhëzues me titull: **"***Si të dallojmë përmbajtjen e dyshimtë online?"*

ETIKA DIGJITALE, TË DREJTAT DHE KUADRI LIGJOR

Veprimtari: Analiza etike e rasteve online

***Qëllimi i veprimtarisë*:** Nxënësit analizojnë situata të ndryshme nga mjedisi digjital, identifikojnë të drejtat dhe parimet etike që cenohen dhe argumentojnë mënyra të përgjegjshme veprimi.

Përshkrimi i veprimtarisë: Veprimtaria nis me paraqitjen nga mësuesi të 3–4 rasteve të shkurtra, të lidhura me situata reale ose të besueshme nga jeta online e të rinjve, si p.sh.:

- publikimi i një fotografie pa leje;
- tallja ose fyerja në grupin e klasës;
- kopjimi i një materiali pa cituar burimin;
- përdorimi i llogarisë së një shoku pa autorizim;
- shpërndarja e një informacioni ose thashethemi në formë "shakaje".

Më pas, nxënësit ndahen në grupe dhe secili grup analizon një rast duke iu përgjigjur disa pyetjeve udhëzuese:

- Cilat të drejta ose parime cenohen në këtë situatë?
- Cilat janë pasojat për personat e përfshirë?
- A kemi të bëjmë vetëm me sjellje të papërshtatshme, apo edhe me një shkelje më të rëndë?
- Si mund të ishte vepruar ndryshe?
- Cila do të ishte zgjidhja më e drejtë dhe më e përgjegjshme?

Në vijim, grupet prezantojnë përfundimet e tyre dhe mbrojnë qëndrimin me argumente. Mësuesi e udhëheq diskutimin drejt kuptimit se etika digjitale nuk lidhet vetëm me rregullat formale, por me përgjegjësinë ndaj vetes, ndaj të tjerëve dhe ndaj pasojave që sjell sjellja online.

Produkti i mundshëm:

- Analizë etike e rastit;
- Rekomandime për sjellje të drejtë dhe të përgjegjshme në mjedisin digjital.

Veprimtari: Karta e të drejtave dhe përgjegjësive digjitale të klasës

Qëllimi i veprimtarisë: Nxënësit formulojnë parime të përbashkëta për sjelljen e përgjegjshme në mjedisin digjital, duke i lidhur ato me të drejtat, përgjegjësitë dhe etikën e komunikimit online.

Përshkrimi i veprimtarisë: Veprimtaria zhvillohet pasi nxënësit kanë diskutuar çështje që lidhen me privatësinë, pëlqimin për publikim, respektin, të drejtën e autorit, komunikimin etik dhe raportimin e përmbajtjeve të dëmshme. Mësuesi hap diskutimin me pyetjen: *"Cilat parime duhet të respektojmë si klasë në mjedisin digjital?"*

Në vijim, nxënësit punojnë në grupe dhe secili grup propozon 3–4 parime ose rregulla që i konsideron të domosdoshme për përdorimin e përgjegjshëm të teknologjisë dhe komunikimit online në kontekstin shkollor. Për secilin propozim, grupi duhet të argumentojë:

- pse ky parim është i rëndësishëm;
- cilën të drejtë ose përgjegjësi mbron;
- si ndihmon në krijimin e një mjedisi digjital më të sigurt dhe më të respektueshëm.

Pas prezantimit të propozimeve, klasa diskuton formulimet, përzgjedh ato që konsiderohen më të rëndësishme dhe harton një kartë të përbashkët me parime të qarta për sjelljen në mjedisin digjital shkollor. Në përfundim, karta mund të vendoset në klasë ose në një hapësirë të përbashkët të shkollës, si një marrëveshje e përbashkët mbi sjelljen dhe përgjegjësinë digjitale.

Produkti i mundshëm:

- Karta e të drejtave dhe përgjegjësive digjitale të klasës;
- Poster ose dokument i përbashkët për mjedisin e klasës ose të shkollës.

Veprimtari: Debat

Qëllimi i veprimtarisë: Nxënësit analizojnë kufirin ndërmjet lirisë personale në mjedisin digjital, përgjegjësisë ndaj të tjerëve dhe rolit të shkollës në trajtimin e sjelljeve problematike online.

Përshkrimi i veprimtarisë: Veprimtaria nis me paraqitjen nga mësuesi të temës së debatit: ***"A duhet të ketë shkolla të drejtë të ndërhyjë kur sjellja online e një nxënësi dëmton të tjerët, edhe nëse ajo ndodh jashtë mjedisit shkollor?"***

Në hyrje, mësuesi shpjegon shkurt kontekstin e debatit, duke theksuar se në mjedisin digjital kufiri ndërmjet jetës private dhe ndikimit publik nuk është gjithmonë i qartë. Më pas, klasa ndahet në dy grupe:

- Grupi PRO, i cili do të mbrojë qëndrimin se shkolla duhet të ndërhyjë;
- Grupi KUNDËR, i cili do të mbrojë qëndrimin se kjo ndërhyrje duhet të ketë kufij të qartë.

Secili grup punon për të ndërtuar argumentet e veta, duke u mbështetur në pyetje si:

- Cilat të drejta dhe përgjegjësi preken në këtë rast?
- Ku mbaron liria personale dhe ku fillon cenimi i tjetrit?
- Cili është roli i shkollës në mbrojtjen e nxënësve?
- A duhet të ketë kufij ndërhyrja e shkollës në jetën digjitale të nxënësve?
- Cilat mund të jenë pasojat e mungesës së reagimit?

Gjatë përgatitjes, secili grup përcakton:

- argumentet kryesore;
- kundërargumentet e mundshme;
- shembuj ose situata mbështetëse;
- një përfaqësues ose disa folës për prezantimin.

Më pas zhvillohet debati, ku secili grup paraqet argumentet e veta, kundërshton qëndrimin e grupit tjetër dhe u përgjigjet pyetjeve apo reagimeve të ngritura gjatë diskutimit. Në fund, të dy grupet përmbledhin qëndrimin e tyre përfundimtar. Mësuesi ose një grup i vogël nxënësish mund të marrë rolin e jurisë dhe ta vlerësojë debatin mbi bazën e qartësisë së argumenteve, përdorimit të shembujve, forcës së kundërargumenteve, respektimit të rregullave të debatit dhe qëndrueshmërisë logjike të pozicionit të mbajtur. Në përfundim, evidentohen pikat më të forta të secilit grup dhe shpallet grupi fitues, ndërsa klasa reflekton shkurt mbi çfarë mësoi në lidhje

me etikën digjitale, përgjegjësinë personale dhe kufijtë e ndërhyrjes institucionale në mjedisin online.

REAGIMI NDAJ INCIDENTEVE DHE HIGJIENA KIBERNETIKE

Veprimtari: Simulimi i reagimit ndaj incidentit

***Qëllimi i veprimtarisë*:** Nxënësit analizojnë incidente të ndryshme digjitale dhe planifikojnë hapat që duhen ndërmarrë për reagim të sigurt, të shpejtë dhe të arsyetuar.

Përshkrimi i veprimtarisë: Veprimtaria nis me paraqitjen nga mësuesi të disa skenarëve të sigurt për analizë, si p.sh.:

- "Llogaria ime po dërgon mesazhe pa dijeninë time";
- "Kam humbur telefonin";
- "Mora një mesazh kërcënues";
- "Klikova aksidentalisht një lidhje të dyshimtë".

Nxënësit ndahen në grupe dhe secili grup punon mbi një skenar të caktuar. Detyra e tyre është të ndërtojnë një plan reagimi të organizuar në tri faza:

- çfarë duhet bërë në 10 minutat e para;
- çfarë duhet bërë brenda ditës;
- çfarë duhet bërë më pas për të rikuperuar situatën dhe për të ulur rrezikun në të ardhmen.

Gjatë punës, nxënësit marrin në konsideratë veprime si ruajtja e qetësisë, ndërrimi i fjalëkalimit, aktivizimi i mbrojtjes shtesë, ruajtja e provave, bllokimi ose raportimi, si dhe komunikimi me një të rritur të besuar ose me shkollën. Në vijim, grupet prezantojnë planin e tyre të reagimit dhe argumentojnë pse e konsiderojnë atë të përshtatshëm. Mësuesi përmbledh hapat kryesorë dhe thekson rëndësinë e reagimit të shpejtë, të strukturuar dhe të mbështetur në vendime të arsyetuara.

Produkti i mundshëm:

- Skemë reagimi për secilin incident;
- Paraqitje e shkurtër e planit të reagimit.

Veprimtari: Udhërrëfyesi i raportimit dhe kërkimit të ndihmës

Qëllimi i veprimtarisë: Nxënësit identifikojnë burimet e ndihmës dhe të raportimit në rastet e problemeve online dhe ndërtojnë një udhërrëfyes praktik për kërkimin e mbështetjes.

Përshkrimi i veprimtarisë: Veprimtaria nis me një pyetje të drejtpërdrejtë nga mësuesi: **"***Nëse përballesh me një problem serioz online, kujt do t'i drejtohesh fillimisht?*" Përmes një diskutimi

të shkurtër, nxënësit evidentojnë burimet e mundshme të ndihmës në familje, në shkollë, në platforma dhe në institucione të tjera mbështetëse.

Më pas, nxënësit punojnë në grupe dhe ndërtojnë një hartë raportimi dhe mbështetjeje, ku përfshijnë:

- personat e besuar në familje;
- mësuesin, psikologun ose drejtuesit në shkollë;
- mekanizmat e raportimit në platformat digjitale;
- burime të tjera ndihme për raste të ngacmimit, shantazhit, presionit emocional ose përmbajtjeve shqetësuese.

Në vijim, secili grup organizon informacionin në formën e një udhërrëfyesi të shkurtër dhe të kuptueshëm për bashkëmoshatarët, me hapa të qartë për atë se çfarë duhet bërë dhe kujt duhet t'i drejtohen në situata të ndryshme problematike online.

Pas prezantimeve, mësuesi përmbledh idetë kryesore dhe thekson se kërkimi i ndihmës nuk është shenjë dobësie, por veprim i përgjegjshëm dhe mbrojtës.

Produkti i mundshëm:

- Hartë raportimi dhe mbështetjeje;
- Udhërrëfyes i shkurtër me titull: **"***Kujt t'i drejtohem kur kam një problem online?"*

Veprimtari: Plani im i reagimit ndaj incidenteve digjitale

Qëllimi i veprimtarisë: Nxënësit hartojnë një plan personal ose familjar për reagimin ndaj incidenteve digjitale, duke e lidhur të nxënin me situata konkrete të jetës së përditshme.

Përshkrimi i veprimtarisë: Në këtë veprimtari, secili nxënës punon individualisht dhe plotëson një model të thjeshtë plani personal ose familjar, ku përfshin:

- kontaktet e ndihmës;
- veprimet prioritare në rast incidenti;
- të dhënat që duhen ruajtur;
- mënyrat e rikuperimit të llogarive ose pajisjeve;
- rregulla të thjeshta për privatësinë dhe kontrollin periodik të sigurisë.

Përpara plotësimit të planit, mësuesi rikujton shkurt disa nga parimet kryesore të trajtuara në tematikë, si rëndësia e ruajtjes së provave, raportimit në kohë, mbrojtjes së llogarive dhe kujdesit të vazhdueshëm ndaj pajisjeve dhe të dhënave personale. Në përfundim, nxënësit reflektojnë në mënyrë të shkurtër mbi rëndësinë e të qenit të përgatitur për situata të papritura në mjedisin digjital.

Produkti i mundshëm:

- Plan personal ose familjar i reagimit ndaj incidenteve digjitale.

Veprimtari: Ku raportoj? Harta e burimeve të ndihmës dhe raportimit

Qëllimi i veprimtarisë: Nxënësit njohin burimet konkrete të ndihmës dhe të raportimit në Shqipëri për situata problematike në mjedisin digjital dhe mësojnë të dallojnë se ku duhet të drejtohen në varësi të natyrës së rastit.

Përshkrimi i veprimtarisë: Veprimtaria nis me një pyetje hyrëse nga mësuesi: **"***Nëse përballesh me një problem serioz online, a mjafton vetëm ta bllokosh apo duhet edhe ta raportosh? Dhe ku?***"** Mbi këtë pyetje zhvillohet një diskutim i shkurtër, ku nxënësit ndajnë mendime dhe përvoja mbi mënyrat e kërkimit të ndihmës.

Më pas, mësuesi paraqet disa raste të ndryshme, si p.sh.:

- marrja e një mesazhi kërcënues;
- përballja me bullizëm kibernetik;
- shpërndarja e një fotografie pa leje;
- ekspozimi ndaj përmbajtjes së papërshtatshme;
- raportimi i përmbajtjes problematike në media ose platforma online.

Në vijim, nxënësit ndahen në grupe dhe secili grup analizon rastet duke u përpjekur të përcaktojë:

- kur duhet të kërkohet ndihmë;
- kujt duhet t'i drejtohet nxënësi fillimisht;
- cili institucion ose shërbim është më i përshtatshëm për raportim;
- çfarë informacioni duhet të ruhet ose të përgatitet përpara raportimit.

Mësuesi i orienton nxënësit drejt njohjes së disa burimeve konkrete, si:

- **ALO 116 / 116 111**, si linjë ndihme dhe mbështetjeje për fëmijët dhe adoleshentët;
- **I SIGURT / Raporto**, si platformë për raportimin e incidenteve dhe përmbajtjeve problematike në internet;
- **AMA**, për rastet që lidhen me përmbajtje të papërshtatshme ose problematike në media audiovizive.

Pas diskutimit, secili grup ndërton një *hartë të shkurtër të raportimit*, ku lidh llojin e problemit me burimin konkret të ndihmës ose institucionin ku mund të drejtohet përdoruesi. Në fund, grupet prezantojnë hartat e tyre dhe klasa ndërton një version të përbashkët, i cili mund të përdoret si material orientues për nxënësit.

Produkti i mundshëm:

- Hartë e burimeve të ndihmës dhe raportimit;

- Udhërrëfyes i shkurtër me titull: “Ku raportoj kur kam një problem online?”

PROJEKT FINAL DHE NDËRGJEGJËSIM NË KOMUNITET

Veprimtari: Zgjedhja e temës dhe planifikimi i projektit

Qëllimi i veprimtarisë: Nxënësit përzgjedhin një temë me interes për komunitetin shkollor dhe planifikojnë në mënyrë të strukturuar realizimin e projektit final.

Përshkrimi i veprimtarisë: Veprimtaria nis me një diskutim të shkurtër, ku mësuesi orienton nxënësit të reflektojnë mbi çështjet e sigurisë kibernetike dhe qytetarisë digjitale që kanë më shumë rëndësi për komunitetin e tyre shkollor. Në këtë kuadër, nxënësit propozojnë tema të mundshme, si siguria e fjalëkalimeve, privatësia në rrjetet sociale, verifikimi i informacionit, bullizmi kibernetik, higjiena digjitale ose reagimi ndaj incidenteve.

Më pas, nxënësit ndahen në grupe dhe secili grup përzgjedh një temë të caktuar. Nën udhëheqjen e mësuesit, grupet planifikojnë projektin duke përcaktuar:

- qëllimin e projektit;
- audiencën së cilës do t’i drejtohen;
- formatin e produktit që do të realizojnë;
- ndarjen e roleve dhe përgjegjësive brenda grupit;
- burimet që do të përdorin.

Në përfundim, secili grup paraqet shkurt planin e vet para klasës dhe merr sugjerime për përmirësim nga mësuesi dhe bashkëmoshatarët.

Produkti i mundshëm:

- Skicë-projekt me temën, qëllimin, audiencën, formatin e produktit dhe ndarjen e roleve.

Veprimtari: Hartimi dhe realizimi i produktit final

Qëllimi i veprimtarisë: Nxënësit realizojnë në grup një produkt final me vlerë ndërgjegjësuese, duke zbatuar njohuritë dhe aftësitë e fituara gjatë modulit.

Përshkrimi i veprimtarisë: Në këtë fazë, grupet punojnë për realizimin e produktit të përzgjedhur, i cili mund të marrë forma të ndryshme, si poster informues, guidë praktike, video e shkurtër, podcast, prezantim, stendë ndërgjegjësuese, fletëpalosje, mini-workshop ose fushatë informuese në mjedisin e shkollës. Gjatë punës, nxënësit organizojnë përmbajtjen, përzgjedhin mesazhet kryesore dhe vendosin mënyrën më të përshtatshme për t’i paraqitur ato te audienca e synuar. Mësuesi ndjek procesin, jep komente dhe orientime për:

- saktësinë e përmbajtjes;
- qartësinë e mesazhit;

- strukturën e produktit;
- etikën e komunikimit;
- përshtatshmërinë e produktit për audiencën.

Në vijim, grupet rishikojnë produktin mbi bazën e sugjerimeve të marra dhe përgatisin versionin përfundimtar për prezantim.

Produkti i mundshëm:

- Produkt final i grupit, i gatshëm për prezantim.

Veprimtari: Prezantimi publik dhe reflektimi

Qëllimi i veprimtarisë: Nxënësit prezantojnë produktin final, argumentojnë zgjedhjet e tyre dhe reflektojnë mbi procesin e punës dhe mbi njohuritë e fituara gjatë modulit.

Përshkrimi i veprimtarisë: Produktet përfundimtare prezantohen përpara klasës, një audience më të gjerë shkollore ose në një aktivitet të dedikuar në nivel shkolle. Gjatë prezantimit, secili grup shpjegon:

- temën e zgjedhur;
- arsyen pse e konsideroi të rëndësishme;
- mesazhin kryesor që synon të përcjellë;
- mënyrën si e ka ndërtuar produktin.

Pas prezantimeve, zhvillohet një diskutim i shkurtër reflektues, ku nxënësit ndalen te pyetje si:

- Çfarë mësuam gjatë këtij moduli?
- Çfarë ndryshon në mënyrën si e përdorim teknologjinë?
- Cilat njohuri ose aftësi na duken më të dobishme për jetën reale?
- Si mund të përdoret më tej ky produkt në shkollë?

Reflektimi mund të zhvillohet me gojë, përmes një flete vetëvlerësimi ose me komente të shkurtra nga bashkëmoshatarët. Në përfundim, mësuesi përmbledh vlerën e punës së realizuar dhe evidenton kontributin e nxënësve në ndërgjegjësimin e komunitetit shkollor.

Produkti i mundshëm:

- Prezantim publik i projektit;
- Reflektim individual dhe feedback nga bashkëmoshatarët.

8. PRODUKTI FINAL I MODULIT

Në përfundim të modulit, nxënësit realizojnë një produkt përfundimtar në grup, i cili pasqyron në mënyrë të integruar njohuritë, aftësitë dhe qëndrimet e zhvilluara gjatë gjithë procesit mësimor.

Produkti final synon të lidhë të nxënit me situata reale dhe të nxisë angazhimin aktiv të nxënësve në rritjen e ndërgjegjësimit për sigurinë kibernetike dhe qytetarinë digjitale në komunitetin shkollor. Përmes këtij produkti, nxënësit jo vetëm konsolidojnë njohuritë e fituara gjatë modulit, por edhe i zbatojnë ato në mënyrë konkrete, duke përcjellë mesazhe të qarta, të sakta dhe të dobishme për bashkëmoshatarët dhe për komunitetin e shkollës.

Produkti final mund të marrë forma të ndryshme, në varësi të temës së përzgjedhur dhe të organizimit të punës në grup, si p.sh.:

- **poster informues ose infografik**, me mesazhe ndërgjegjësuese për sigurinë e llogarive, privatësinë, verifikimin e informacionit ose reagimin ndaj incidenteve digjitale;
- **guidë praktike ose fletëpalosje**, me këshilla dhe hapa konkretë për përdorim të sigurt dhe të përgjegjshëm të teknologjisë;
- **video e shkurtër, podcast, prezantim ose mini-fushatë ndërgjegjësuese**, e ndërtuar mbi situata, raste ose tema të trajtuara gjatë modulit;
- **stendë informuese ose veprimtari sensibilizuese në shkollë**, e organizuar për nxënës të tjerë ose për komunitetin shkollor.

Gjatë realizimit të produktit final, nxënësit punojnë në grup, ndajnë role dhe përgjegjësi, përzgjedhin burime të besueshme, strukturojnë përmbajtjen dhe kujdesen që mesazhi i tyre të jetë i saktë, etik, i kuptueshëm dhe i përshtatshëm për audiencën së cilës i drejtohen.

Produktet mund të prezantohen në klasë, në një aktivitet të përbashkët në nivel shkolle ose në kuadër të një nisme ndërgjegjësuese të organizuar nga vetë nxënësit. Produktet më përfaqësuese mund të ekspozohen në mjediset e shkollës ose të përdoren si materiale informuese për bashkëmoshatarët.

Në këtë mënyrë, produkti final shërben jo vetëm si përmbyllje e modulit, por edhe si një formë e zbatimit praktik të njohurive dhe si kontribut konkret i nxënësve në promovimin e një kulture më të sigurt dhe më të përgjegjshme digjitale.

Shënim: *Nëse moduli zhvillohet në kuadër të kurrikulës me bazë shkolle, ai nuk vlerësohet me notë dhe shënohet si shlyerje. Nëse shkolla përzgjedh ta zhvillojë modulin në kuadër të kurrikulës me zgjedhje, atëherë ai vlerësohet me notë, në përputhje me kriteret në fuqi për vlerësimin e nxënësve në arsimin parauniversitar.*